Research Proposal

CST 395-2 Research Methodology and Scientific Writing

This proposal is submitted in partial fulfillment of the requirements for the degree of

Bachelor of Science Honours in Computer Science and Technology

Group 01

Your Research Title Here

Supervised by

Dr. Initials1 Surname1

Mr. Initials2 Surname2

Ms. Initials3 Surname3

Department of Computer Science and Informatics

Faculty of Applied Sciences

Uva Wellassa University of Sri Lanka

July 23, 2025

Proposed Title

Your Research Title Here

Students Agreement

By signing below on _ , we, as Group _ _ _ _ members, agree to the terms of the CST 395-2 Research Methodology and Scientific Writing course at the 300 level. We commit to conducting the research project titled as mentioned above and outlined in the agreement. We understand that any changes to the group composition, identified research problem, or selected supervisor may result in penalties.

Name	**Registration Number**	**Signature**
Mr. Initials1 Surname1	UWU/CST/20/001	
Ms. Initials2 Surname2	UWU/CST/20/002	
Mr. Initials3 Surname3	UWU/CST/20/003	
Ms. Initials4 Surname4	UWU/CST/20/004	

Supervisor Agreement

I/We agree to supervise the above group of students throughout their research project, providing guidance and support for successful completion. I/We acknowledge that changes to group composition, identified research problem, or responsibilities may require further discussion.

Name	**Signature**	**Date**
Dr. Initials1 Surname1		
Mr. Initials2 Surname2		
Ms. Initials3 Surname3		

Contents

List of Figures

List of Tables

List of Abbreviations

AI	Artificial Intelligence
ANN	Artificial Neural Networks
API	Application Programming Interface

1 Introduction

1.1 Background of the Study

Provide background information about your research topic. Use citations appropriately.

Example:

Let's assume a research study titled 'A Reinforcement Learning Approach for Phishing Detection.'

With the rapid expansion of internet services, the need for effective cybersecurity has become more critical than ever. As individuals and organizations increasingly rely on digital platforms for communication, transactions, and data storage, the risk of cyber threats has grown proportionally. Among various cyberattacks, social engineering techniques—especially phishing—have emerged as a prevalent and damaging form of attack, capable of deceiving even experienced users into revealing sensitive information.

Phishing attacks are designed to trick users into providing personal credentials such as usernames, passwords, and financial information, typically through fraudulent emails or websites that mimic legitimate ones. These attacks are often difficult to detect due to their dynamic nature and the ever-evolving tactics used by attackers. Traditional phishing detection techniques, which rely heavily on blacklists or rule-based systems, often fail to keep up with zero-day threats or previously unseen attack patterns.

To overcome these limitations, machine learning approaches have been increasingly applied to phishing detection. While supervised learning has shown promise, it depends on large volumes of labeled data and may struggle with adapting to new patterns in phishing behavior. Recent research interest has turned toward reinforcement learning (RL) — a learning paradigm that enables models to improve through interaction with their environment. RL-based systems can potentially learn to detect phishing websites by sequentially exploring and evaluating features, offering adaptability and decision-making in uncertain or changing conditions. However, despite its theoretical potential, the application of RL in phishing detection remains limited and underexplored.

Given the dynamic nature of phishing attacks and the adaptability required to detect them effectively, this study aims to investigate the feasibility and performance of reinforcement learning techniques in phishing website detection. By developing and eval-

uating an RL-based model, the research seeks to contribute a novel, adaptive solution that addresses the shortcomings of traditional and supervised learning approaches. The findings of this study may offer insights into how intelligent agents can be used to improve real-time threat detection and cybersecurity resilience.

1.2 Problem Statement

Clearly state the research problem that your study aims to address.

Para 1: Start by briefly explaining the broader area of your research. Provide context and explain why this domain is important or relevant today. Mention any current trends, challenges, or real-world importance to set the stage. Narrow the focus to a particular issue or gap within the broader area. Clearly state what is lacking, ineffective, or not well understood. Show why this problem matters. Describe what negative outcomes may occur if the issue is not addressed.

Para 2: Mention what previous researchers or systems have done and explain where they fall short. Identify any areas that have not been fully explored or problems that existing methods do not adequately solve.

Para 3: Summarize the problem in a clear way. Clearly communicate what the issue is, why it is significant, and why it needs to be studied now. This final paragraph becomes your official problem statement. (This paragraph is what you wrote during Lesson 3.)

Use citations where necessary.

1.3 Aim, Objectives and Questions

Explain the aim of your research. List the specific objectives of your study. State any hypotheses you plan to test (if applicable). List research questions that your study seeks to answer.

- Aim: Aim goes here.
- Objectives:
  - Objective 1 goes here.
  - Objective 2 goes here.
  - Objective 3 goes here

system.

- Research Questions:
  - Question 1 goes here
  - Question 2 goes here
  - Question 3 goes here

1.4 Rationale of the Study

Explain why you are doing this research or why the study is needed.

1.5 Significance of the Study

Explain why the results are important. Think from academic and social perspectives.

1.6 Scope and Limitations of the Study

Define the boundaries of your research by outlining the specific aspects or areas it will cover. Additionally, mention any limitations or constraints that may impact the extent or depth of your study.

2 Literature Review

First, give a small introduction to the section.

Arrange your related literature in Thematic or Chronological approach. Better to follow Thematic approach.

Summarize what was found and clearly identify the gap your research will fill - this will be a separate sub-section and the last section

Use citations appropriately.

Here is an example reference using Harvard style: (Chiew et al. 2018).

Also, you can use it in this way as well: Chiew et al. (2018) stated that ...

Let's assume a research study titled 'A Reinforcement Learning Approach for Phishing Detection.' If a thematic approach is used, the following themes can be considered, and these will serve as the sub-sections of this section.

2.1 Overview of Phishing Attacks

2.2 Traditional Phishing Detection Techniques

2.3 Machine Learning Approaches for Phishing Detection

2.4 Reinforcement Learning in Cybersecurity

2.5 Gaps in the Existing Literature

3 Research Methodology

First, give a small introduction to the section - briefly mention your philosophical things here (e.g., positivism, pragmatism)

3.1 Research Approach and Strategy

Explain whether your study will adopt a qualitative, quantitative, or mixed methods approach. Justify your choice based on the nature of your research questions and objectives.

3.2 Data Collection Methods

Outline the methods you will use to collect data. This may include surveys, interviews, observations, experiments, or archival research. Explain why these methods are appropriate for your study.

3.3 Sampling Strategy

Describe your sampling strategy, including the population or sample size, sampling technique, and any inclusion or exclusion criteria. Justify your sampling decisions based on the characteristics of your target population and the objectives of your study.

3.4 Data Analysis Techniques

Explain the analytical techniques you will use to analyze your data. This may include statistical analysis, thematic analysis, content analysis, or other qualitative or quantitative methods. Justify your choice of analysis techniques based on the nature of your data and research questions.

3.5 Ethical Considerations

Discuss any ethical considerations related to your research, such as informed consent, confidentiality, privacy, and potential risks to participants. Explain how you will address these ethical concerns to ensure the welfare of participants and the integrity of your study.

3.6 Evaluation Strategy

Describe metrics, baseline comparisons, validations, tools/frameworks, and how success is planned to measure.

3.7 Tools and Technologies

Mention specific tools, platforms, libraries, and hardware planned to use.

4 Proposed Timeline

You can use a Gantt chart to visually represent the timeline. Common tasks are listed below; however, you have full freedom to adjust these tasks according to your study. When drawing the Gantt chart, make sure to pin the points where you achieve the objectives.

- Proposal Writing & Approval
- Literature Review
- Dataset Collection or Preprocessing
- Model/Framework Development
- Evaluation & Testing
- Analysis & Discussion
- Documentation

You can use the time period from this semester to the second semester of Level 400, since you have started your research work in this semester.

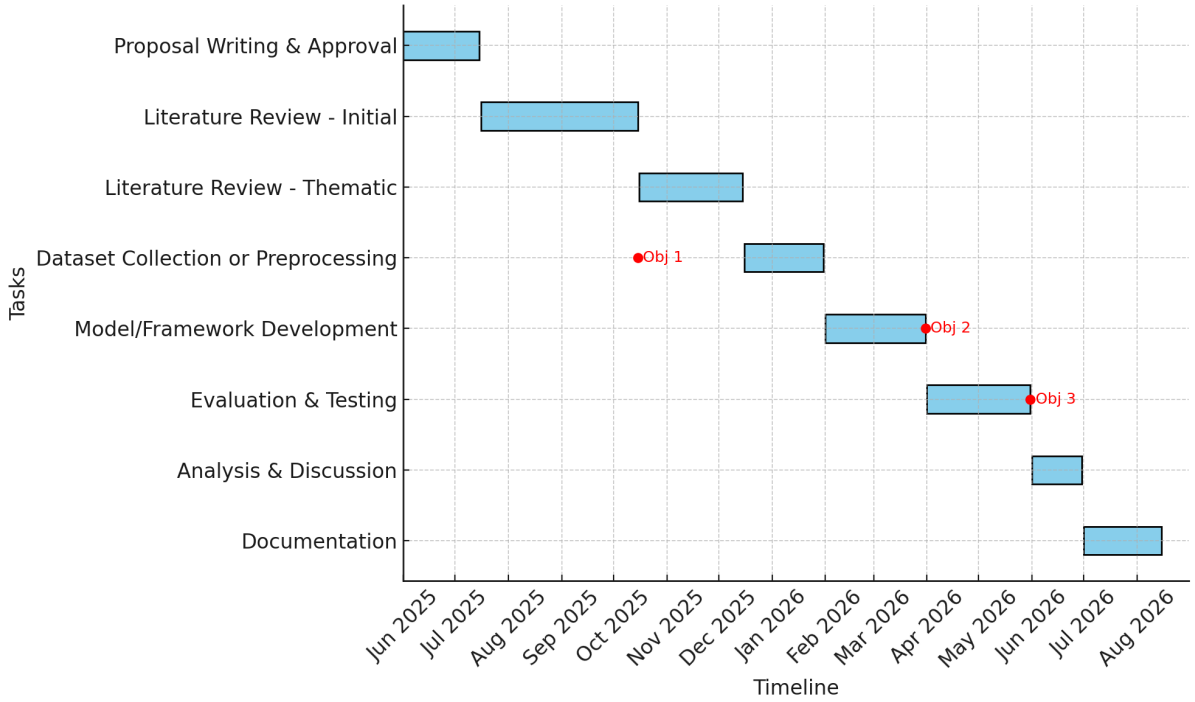

Figure 1: Project Plan

5 Expected Outcomes

Main deliverables – A model, a prototype, a framework, etc.

What new understanding or knowledge will your research add?

How can others use your findings?

Will it help future researchers?

How objectives are met? – mention the specific deliverables that will be produced as a result of achieving each objective

References

Chiew, K. L., Yong, K. S. C. & Tan, C. L. (2018), 'A survey of phishing attacks: Their types, vectors and technical approaches', *Expert Systems with Applications* **106**, 1–20. **URL:** *https://doi.org/10.1016/j.eswa.2018.03.050*